

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Patent Examiner:

Hidema Tanaka et al.

Group Art Unit:

Serial No.: 10/762,653

Filed: January 21, 2004

April 13, 2004

For: CIPHE

CIPHER STRENGTH EVALUATION

APPARATUS

Irvine, California 92614

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450

Dear Sir:

In an attempt to fully comply with the duty of disclosure set forth in 37 C.F.R. § 1.56 and in conformance with 37 C.F.R. §§ 1.97 and 1.98, applicant wishes to bring to the attention of the U.S. Patent Office the following references:

S.Moriai, T.Shimoyama, T.Kaneko, "Higher Order Attack of a CAST Cipher", Fast Software Encryption 1998, FSE-4th, LNCS.1372. 1998.

T.Shimoyama, S.Moriai, T.Kaneko and S.Tsuji, "Improved Higher Order Differential Attack and Its Application to Nyberg-Knudsen's Designed Block Cipher", IEICE TRANS. FUNDAMEN TALS, VOL.E82-A, NO 9 pp 1971-1980, 1999.

M.Matsui,"New Block Encryption Algorithm MISTY, "Fast Software Encryption 1997 FSE 1997, pp 54-67, 1997.

H.Tanaka, T.Kaneko, "An Attack of 6-round MISTY1 without FL functions", TECHMCALREPORT OF IEICE, pp. 53-59, 2002.

Copies of these references and a form PTO-A820 are attached.

If the Examiner believes that a telephone conference would help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to:
Commissioner for Patent, PO Box 1450,
Alexandria, VA 22313-1450 on April 13, 2004

by: James Lee

Signature

Date of Signature: April 13, 2004

Very truly yours,

SNELL & WILMER LLP

Joseph W. Price, Esq.

Reg. No. 25,124

1920 Main Street, Suite 1200

Irvine, CA 92614 Phone 949/253-4920

O 1 P INFORMATION DISCLOSURE CITATION			43521-160	0	SERIAL NO. 10/762,653			
Use several sheets if necessary)				Hidema Tanaka et al. FILING GROUP				
141.11	Ħ			01/21/2004	4			
EXAMINEA E	25		U.S. P	ATENT DOCUMENTS				
EXAMINEALE INITIAL	. (DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
3								
							,	
•		-						
}							***	
			FOREIGN	PATENT DOCUMENTS	<u> </u>			
	C	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES NO	
		OTHER DOCUME	ENTS (Including A	Author, Title, Date, Pertinen	t Pages, Etc	;.)		
	SL	.Moriai, T.Shimoyama NCS. 1372. 1998.	a, T.Kaneko, "Highe	r Order Attack of a CAST Cip	her", Fast So	ftware Encrypti	ion 1998, FSE-4th,	
	T	Shimoyama, S.Moria lyberg-Knudsen's Desi	i, T.Kaneko and S.T. gned Block Cipher"	suji,"Improved Higher Order , IEICE TRANS. FUNDAMEN	Differential A TALS, VOL.	Attack and Its A E82-A, NO 9 pp	pplication to 5 1971-1980, 1999.	
EXAMINER				DATE CONSIDERED				
*EXAMINER: I considered. In	nitial if refer clude copy	ence considered, wheth of this form with next co	er or not citation is in ommunication to application	conformance with MPEP 609; Dra ant.	w line through	citation if not in c	conformance and not	

Form PTO-A820 (also form PTO-1449)

INFORMATION DISCLOSURE CITATION

ATTY DOCKET NO. 43521-1600	SERIAL NO. 10/762,653			
Hidema Tanaka et al.				
FILING 01/21/2004	GROUP	Ī		

(Use several sheets if necessary)			Hidema Tanaka et al.				
.00			FILING 01/21/20		ROUP		
		U.S. P/	ATENT DOCUMENTS				
*EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
į			-				
				•			
		·					
		FOREIGN	PATENT DOCUMENTS				
	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
					1	YES NO	
			···				
		·					
					·		
•	OTHER DOCUME	NTS (Including A	uthor, Title, Date, Pertine	nt Pages, Etc.)			
	M.Matsui,"New Block	Encryption Algorithm	n MISTY, "Fast Software En	eryption 1997 FS	SE 1997, pp 54	l-67, 1997.	
	H.Tanaka, T.Kaneko, "pp. 53-59, 2002	An Attack of 6-roun	d MISTY1 without FL functi	ons", TECHMC	ALREPORT (OF IEICE,	

EXAMINER

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.